Approved: _____
ALEXANDER H. SOUTHWELL
Assistant United States Attorney

Before: HONORABLE HENRY B. PITMAN
United States Magistrate Judge
Southern District of New York

- - - - - - - - - - - - - - - - - - - - - x

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | : | **SEALED COMPLAINT** |
| - v. - | : | |
| WILLIAM P. GENOVESE, JR., a/k/a “illwill,” a/k/a “xillwillx@yahoo.com,” | : | Violation of 18 U.S.C. § 1832<br>COUNTY OF OFFENSE: NEW YORK |
| Defendant. | : | |

- - - - - - - - - - - - - - - - - - - - - x

SOUTHERN DISTRICT OF NEW YORK, ss.:

FRANK C. MANZI, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation, and charges as follows:

**COUNT ONE**
**(Unlawful Distribution of Trade Secrets)**

1. From in or about February 2004, up to and including in or about July 2004, in the Southern District of New York, and elsewhere, WILLIAM P. GENOVESE, JR., a/k/a “illwill,” a/k/a “xillwillx@yahoo.com,” the defendant, did knowingly, willfully, and unlawfully, and without authorization, copy, duplicate, download, upload, replicate, transmit, deliver, send, communicate, and convey a trade secret that is related to and included in a product that is produced for and placed in interstate and foreign commerce with the intent to convert that trade secret to the economic benefit of someone other than the owner thereof, and intending and knowing that the offense would injure the owner of the trade secret, to wit, GENOVESE sold and attempted to sell the source code for the computer programs Microsoft Windows NT 4.0 and Windows 2000.

(Title 18, United States Code, Sections 1832(a)(2), 1832(a)(4) and 2).

The bases for my knowledge and for the foregoing charge, is,

in part, as follows:

2. I am a Special Agent with the FBI, and have been employed in that position for approximately three and a half years. I am presently assigned to a squad that investigates criminal offenses involving computer intrusions as well as intellectual property violations, including theft and misappropriation of trade secrets and criminal copyright infringement. Over the past three and a half years I have participated in numerous investigations involving theft of trade secrets and copyright infringement. Based upon my training and experience, I am familiar with at least several of the means by which individuals engage in these offenses. Because this Affidavit is being submitted for the limited purpose of establishing probable cause for the offenses cited above, I have not included every detail of every aspect of the investigation. In addition, the information contained in this Affidavit is based upon my conversations with other law enforcement officers and others, my review of documents and reports prepared by others, and my personal observation and knowledge. Unless specifically indicated otherwise, all conversations and statements described in this Affidavit are related in substance and in part only.

**Background Information From Microsoft**

3. In or about February 2004, I learned from news reports that stolen source code for two Microsoft Corporation programs, Windows 2000 and Windows NT 4.0, were being disseminated over the Internet.

4. In or about February 2004, I received the following information from a representative (the “Representative”) of Microsoft Corporation (“Microsoft”) concerning the theft and unlawful distribution of the source code for Windows 2000 and Windows NT 4.0:

a. Microsoft possesses trade secret rights, and owns copyrights, in its Windows NT 4.0 and Windows 2000 source code. “Source code” is the human-readable code in which software developers write programs. Unlike Microsoft's object code (the machine-readable code that is the format in which Microsoft distributes its software to customers), source code for commercial products like Windows NT 4.0 and Windows 2000 is never released to the public. Microsoft’s source code is considered the “crown jewels” of the company.

b. Both Windows NT 4.0 and Windows 2000 software are “operating systems” - the software that controls the allocation

and usage of hardware resources such as memory, central processing unit (CPU) time, disk space, and peripheral devices. In short, an operating system is the foundation on which all other programs are built. Without an operating system, a computer cannot run e-mail, word processing, or virtually any other application.

c. Both Windows NT 4.0 and Windows 2000 are operating systems that are largely used in business environments. Both Windows NT 4.0 and Windows 2000 have an estimated retail value of $319 per program.

d. Microsoft closely guards its source code – for Windows NT 4.0 and Windows 2000, as well as other programs – as trade secrets. Microsoft strictly controls the distribution of its source code, and provides it to only a limited number of third parties outside the company, such as certain software developers and government agencies. Every recipient of Microsoft's source code is required to sign a strict non-disclosure agreement and license agreement that both expressly prohibits the licensee from distributing the code to others and requires them to employ significant safeguards to protect the confidentiality of the code.

e. On or about February 12, 2004, Microsoft learned that significant portions of the source code for both Windows NT 4.0 and Windows 2000 were misappropriated (the "Stolen Source Code") and unlawfully released onto, and distributed over, the Internet without its authorization.

## The Investigation

### Microsoft's Investigation

5. In or about February 2004, I also learned from the Representative that Microsoft had retained a number of outside vendors and online security firms to investigate the dissemination of the Stolen Source Code over the Internet. I further learned from the Representative that one of those vendors ("the Vendor") identified a Web site known as "illmob.org" that was offering the Stolen Source Code for sale. Specifically, the Vendor located a message on the "illmob.org" Web site posted by a person identified only as "illwill" on or about February 12, 2004, which announced that "illmob.org" had obtained a copy of the Stolen Source Code and that "illwill" would sell the Stolen

Source Code using his "FTP" server.[1]

6. In or about March 2004, I received from the Representative a copy of the investigative report conducted by an online security firm hired by Microsoft (the "Online Security Firm") from which I learned:

a. On or about February 18, 2004, an investigator at the Online Security Firm ("the Investigator") accessed the Web site known as "illmob.org," which was offering to sell the Stolen Source Code. On that Web site, the Investigator observed a contact e-mail address for "illwill" of "xillwillx@yahoo.com" and sent an e-mail to "illwill" asking for a copy of the Stolen Source Code. Later that day, the Investigator received an e-mail response from "xillwillx@yahoo.com" asking for a "donation" to provide access to the Stolen Source Code.

b. On or about February 19, 2004, the Investigator sent another e-mail to "xillwillx@yahoo.com" seeking clarification of the last message from "xillwillx@yahoo.com," specifically asking how much "illwill" was charging for the Stolen Source Code and how to send payment for the Stolen Source Code to "illwill." Later that day, the Investigator received an e-mail response from "xillwillx@yahoo.com" directing the Investigator to a PayPal[2] link on the "illmob.org" Web site but without specifying an amount to be paid for the Stolen Source Code. The Investigator then initiated a payment of $20 to "xillwillx@yahoo.com" through PayPal and sent another e-mail to "xillwillx@yahoo.com" announcing the sending of that payment. Later that day, the Investigator received a response e-mail from "xillwillx@yahoo.com" acknowledging that payment was in process.

c. On or about February 26, 2004, the Investigator learned that his PayPal payment to "xillwillx@yahoo.com" had cleared and the Investigator e-mailed "xillwillx@yahoo.com" notifying him that the payment had cleared and asking for specific directions on how to download the Stolen Source Code. Later that day, the Investigator received an e-mail from "xillwillx@yahoo.com" in which "illwill" instructed the

---

[1] "FTP," or File Transfer Protocol, is a protocol by which clients can transfer files to a server. An FTP server is commonly used to download files from the Internet.

[2] PayPal is an online payment service, which enables any individual or business with an e-mail address to send and receive payments online.

Investigator to access his FTP server ("Illwill's FTP Server") and to use the file name "win2k" and password of "source" in order to download the Stolen Source Code from Illwill's FTP Server.

d. On or about February 28, 2004, another investigator with the Online Security Firm ("Investigator-2"), following the instructions provided by "illwill" described above, downloaded the Stolen Source Code from Illwill's FTP Server, while Investigator-2 was in Manhattan. While downloading the Stolen Source Code, Investigator-2 identified the Internet Protocol ("IP") address[3] for Illwill's FTP Server ("Illwill's FTP IP Address"). After downloading the Stolen Source Code from Illwill's FTP Server, Investigator-2 provided the file he had downloaded to a representative of Microsoft which confirmed that the file contained the Stolen Source Code.

**The FBI's Investigation**

**Obtaining A Copy Of The Stolen Source Code From "Illwill"**

7. In or about July 2004, I asked the Investigator to assist me in obtaining a copy of the Stolen Source Code from Illwill's FTP Server. I learned from the Investigator that he thereafter sent an e-mail to "xillwillx@yahoo.com" asking to obtain the Stolen Source Code again and stating that he made another payment to "illwill" via PayPal as he had previously done. I also learned from the Investigator that after sending this request, he had received a response e-mail from "xillwillx@yahoo.com" in which "illwill" provided the file name "win 2000" and password of "win 2000" for the Investigator to download the Stolen Source Code from Illwill's FTP Server.

8. In or about July 2004, the Investigator provided me with the e-mail response from "xillwillx@yahoo.com" which provided the instructions for obtaining the Stolen Source Code from Illwill's FTP Server, which is described above. Thereafter, I accessed Illwill's FTP Server from an undercover computer located in Manhattan and downloaded the Stolen Source Code, following the instructions from "illwill." I then made two copies of the Stolen Source Code and provided one to Microsoft for authentication purposes.

9. In or about August 2004, I learned from the

[3] An internet protocol address, or "IP address," is a unique numerical address assigned to a particular computer that is connected to the internet during a given session.

Representative that the file I had downloaded from Illwill's FTP Server and provided to Microsoft was in fact a copy of the Stolen Source Code.

**Determining The Identity Of "Illwill"**

10. I have learned from records from the State of Connecticut that WILLIAM P. GENOVESE, JR., a/k/a "illwill," a/k/a "xillwillx@yahoo.com," the defendant, was convicted of eavesdropping, in violation of Connecticut General Statutes Section 53a-189, upon a plea of guilty on or about March 13, 2003 and was sentenced to two years probation. I have also reviewed the affidavit of a Connecticut State Trooper submitted as part of the application for an arrest warrant for GENOVESE on these charges, from which I learned:

a. The eavesdropping charges arose from GENOVESE's unauthorized access in or about 2000 to a number of victims' computers in Connecticut. GENOVESE accomplished this unauthorized access by infecting the victims' computers with a type of virus that allowed him to remotely access the computers. Once he had infected the computers with this virus, GENOVESE accessed the victims' computers, capturing their activities using keylogging software,[4] taking over control of the victims' computers, and sending instant messages to the victims telling them what he was doing. In performing these illegal activities, GENOVESE used the screen names "illwill" and "xxXILLWILLXxx" and admitted to some of the victims that he was GENOVESE.

b. On or about November 20, 2000, in the course of a search of GENOVESE's home, GENOVESE made a number of inclupatory statements to a Detective with the Connecticut State Police Computer Crime and Electronic Evidence Unit, including that he had used the screen names "illwill" and "xxxillwillxxx"[5] in connection with remotely accessing victims' computers without their authorization using a virus program.

11. In the course of my investigation, I determined from an inquiry to a publicly-available database that Illwill's FTP IP Address (at the time detailed above when the Investigator accessed it) was owned by Cox Communications, which I know to be

---

[4] Keylogging software, also known as a keystroke logger, is a program or hardware device that captures every key depression on a computer.

[5] The screen name and e-mail address using "illwill" is also obviously a variant of GENOVESE's first name.

an Internet Service Provider. I have obtained records from Cox Communications related to Illwill's FTP IP Address and learned from those records that it corresponded to a cable modem registered to "William Genovese" at a residence in Meridan, Connecticut. I have also reviewed records obtained from the Connecticut Department of Motor Vehicles and Wachovia bank, which indicate that WILLIAM P. GENOVESE, JR., a/k/a "illwill," a/k/a "xillwillx@yahoo.com," the defendant, lives at the residence in Meridan, Connecticut indicated in the Cox Communications records. In addition, I have reviewed records obtained from Yahoo! related to the "xillwillx@yahoo.com" e-mail address, which also indicate that the account was accessed from Illwill's FTP IP Address, which confirms that the cable modem registered to "William Genovese" was used to access the "xillwillx@yahoo.com" account.

12. I also obtained records from PayPal related to WILLIAM P. GENOVESE, JR., a/k/a "illwill," a/k/a "xillwillx@yahoo.com," the defendant, and learned from those records that: (i) GENOVESE maintains an account at PayPal using the e-mail address "xillwillx@yahoo.com"; (ii) someone using Illwill's FTP IP Address (which corresponded to a cable modem registered to "William Genovese") accessed the PayPal account; and (iii) proceeds of that account were transferred to a bank account at Wachovia in the name of GENOVESE. I also subpoenaed records from Wachovia which confirm that various deposits from PayPal had been credited to GENOVESE's account.

WHEREFORE, deponent prays that an arrest warrant be issued and that the above named defendant be imprisoned or bailed as the case may be.

_____
FRANK C. MANZI
Special Agent
Federal Bureau of Investigation

Sworn to before me this
day of November, 2004.

_____
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK